

犯罪捜査支援のための サイバー・フィジカル統合分析技術

谷 真宏

要 旨

テロや組織犯罪をはじめとする犯罪にサイバー空間が活用されており、国境を越えて世界中に拡大する犯罪活動への対策が急務となっています。特に、サイバー空間を活用した犯罪は、犯罪に関わる人物や組織の特定が難航し、また未然防止も困難であることが指摘されています。本稿では、サイバー空間上の大量のデータを活用し、顔認証や物体認識などのバイオメトリクスや各種解析技術を用いて、犯罪捜査に有用な情報を抽出、統合的に分析する取り組みについて紹介します。



パブリックセーフティ/セキュリティ/サイバー空間/サイバー・フィジカル統合分析
バイオメトリクス/ソフトバイオメトリクス

1. はじめに

インターネットは人々の生活に浸透し、2017年4月の時点で、利用者は世界人口の約半数に達しています¹⁾。特に、昨今のソーシャル・ネットワーキング・サービス(SNS)の爆発的な普及を背景に、日々大量の情報が世界中の人々に共有されています。共有される情報は、テキスト、画像・動画、音声・音楽などのさまざまな形態であり、人々はそれらを日々の生活のなかで活用しています。また、日本においては、インターネットショッピングの利用率が全世代的に上昇しているなど²⁾、インターネットと人々の生活は切り離せないものとなってきています。

インターネットが普及する一方で、サイバー空間を活用した犯罪(サイバー利用犯罪: Cyber-enabled crime)が増加しています。例えば、テロや組織犯罪をはじめとする犯罪の計画や準備にサイバー空間が活用されており、国境を越えて世界中に拡大する犯罪活動への対処が難航していることが社会問題となっています。テロにおいては、動画サイトでのプロパガンダ、SNSを活用したリクルートや諜報活動、極めて匿名性の高いオンラインサイトでの資金や武器調達など多岐にわたり、犯罪が巧妙化しているためです。また、テロのみならず、違法薬物の売買やインター

ネットオークション詐欺などのさまざまな犯罪でサイバー空間が活用されています。例えば、シンガポールにおいては、インターネットショッピング詐欺などのオンライン犯罪が2015年に急増(前年比46.5%増加)して以降、依然として懸念対象となっています^{3) 4)}。

このように、サイバー空間は人々の生活する現実の世界と密接に関わっており、現実の世界であるフィジカル空間と同時にサイバー空間においても安全・安心な社会を構築することが重要です。

本稿では、第2章で捜査支援のためのサイバー・フィジカル統合分析技術に関する研究の概要を紹介し、第3章でその研究を支えるNECの重要な解析技術について述べます。第4章で今後の課題について触れ、最後に本稿をまとめます。

2. 捜査支援のためのサイバー・フィジカル統合分析技術

サイバー空間上に存在する大量のデータを活用し、画像やテキストを解析するための各種技術を適用することで、犯罪捜査などに役立つ情報を抽出して統合的に分析する「サイバー・フィジカル統合分析技術」の研究開発に取り組んでいます。サイバー利用犯罪は、例えば、通信経路を

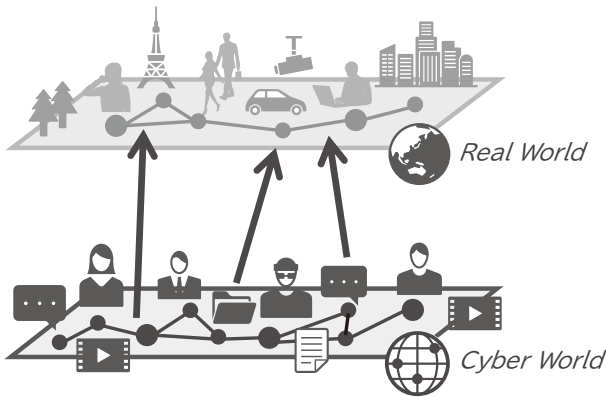


図1 サイバー利用犯罪と実世界情報の関連付け

匿名化するツールが利用されるなど、高度化・複雑化の一途を辿っていますが、特に、このような犯罪を実世界の事象と結びつけることを目指しています(図1)。サイバー空間上には、前述のようにテキスト、画像・動画、音声・音楽などのさまざまな形態の公開情報が大量に存在するため、それらを解析する種々の技術を用いて、サイバー利用犯罪と実世界の事象とを関連付けることのできる情報のみをいかに抽出するかが、重要な研究テーマになると考えています。

具体的には、グローバルな性質を持つサイバー利用犯罪をはじめとするさまざまな犯罪の捜査において、容疑者や行方不明者など目的とする人物の居場所の絞り込みが、1つの重要な課題となっています。例えば、目的の人物が撮影された写真があったとしても、その写真の撮影場所を特定することは容易ではありません。しかし、その人物が着用している衣服や所持品などの商品の販売国や販売地域が分かれば、撮影場所をある程度絞り込むことができる可能性があります。また、背景に写り込んだ建物を特定できれば、更に撮影場所を絞り込むことができます。本研究は、サイバー空間上の画像などの公開情報から、各種解析技術を活用し、このような被写体に係る情報を抽出することによる法執行機関の捜査支援を目的としています。

3. 本研究を支える重要な要素技術

3.1 バイオメトリクス

サイバー空間上の画像や動画などの公開情報から直接的に容疑者や行方不明者などの目的の人物を探し出す場

合、バイオメトリック認証技術が有効な手段になってきます。NECは、指紋認証や顔認証に代表されるバイオメトリクスの研究開発に長年にわたり取り組んでいます。特に、NECの顔認証技術は、米国国立標準技術研究所(NIST)が主催する顔認証技術のベンチマークテストで4回連続の世界トップ性能評価を獲得しており、その製品は世界40カ国100システム以上に導入されている実績があります⁵⁾。また、インターネット上に動画を投稿することによる犯行声明などでは音声も貴重な情報であり、音声から人物を特定する話者認識技術を活用することができます。NECは、顔認証と同様、話者認識の研究開発にも精力的に取り組んでおり、音声による大規模データベース検索が官公庁で実用化されています⁶⁾。

3.2 ソフトバイオメトリクス

目的の人物の顔などのバイオメトリック特徴が得られない場合、ソフトバイオメトリクスが人物やその居場所の絞り込みに有用です。ソフトバイオメトリック特徴は、個人を特徴付ける情報ですが、その情報のみで個人を特定するには弁別性が十分でない情報を指し、例えば、髪の色や肌の色、タトゥー(刺青)、身に付けている衣服やアクセサリなどです。また、目的の人物と関わりのある場所も広義のソフトバイオメトリック特徴ととらえることができます。頻繁に訪れる場所などの日常生活における活動範囲は、少ないながらも個人性を含むと考えられるためです。NECは、独自に開発したコンパクトな画像特徴量に基づき、速度と精度を



(a) タワーの照合

(b) 建物の照合

図2 ソフトバイオメトリクスの実験結果一例

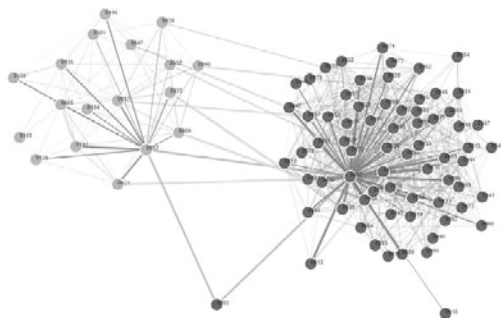


図3 アカウントの関連性分析

高いレベルで両立する物体認識技術を保有しており⁷⁾、これをソフトバイオメトリクスに適用しました。図2にソフトバイオメトリクスの実験結果の一例を示します。図2の(a)は、タトゥー照合結果の一例で、上下の画像間で画像特徴の類似する点が直線で結ばれています。図2の(b)は、建物などの景色を照合した結果の一例です。上の画像のみからその撮影場所を特定することは、一般にその景色に見覚えがなければ困難です。しかし、下の画像と紐付けることができれば、NECのロゴから、上の画像はNECの建物周辺で撮影されたことが分かります。

ソフトバイオメトリクスを応用して、インターネット上のアカウントを関連付ける研究にも取り組んでいます(図3)。目的とする人物が複数のアカウントを保持している場合、同一人物として関連付けることができれば、複数のアカウントに点在する画像やテキストなどの情報を集約し、目的の人物やその交友関係などをより詳細に分析できるためです。関連付けには、例えば、投稿文の文体や内容をはじめとするさまざまな特徴を使用することができます。

NECは、国際的な法執行機関などとともに、ソフトバイオメトリクスの適用可能性について検討を進めています。

4. 取り組むべき課題

これまで技術的な取り組みについて述べてきましたが、実際に法執行機関がこれら技術を使用する場合は、各国の法律に準ずる必要があります。犯罪と無関係なインターネット上のユーザーやそのデータは、公開情報であったとしても保護されなければならないためです。NECは各国の法執行機関と協議しながら、セキュリティとプライバシーのバランスを検討し、安全・安心な社会を実現していきます。

5. むすび

本稿では、サイバー空間上の画像などの大量なデータを活用し、顔認証や物体認識をはじめとする各種解析技術により法執行機関の犯罪捜査を支援するための研究開発について紹介しました。匿名性が高く、かつグローバルなサイバー利用犯罪を、いかに現実世界の事象と関連付けるかが、急増するサイバー利用犯罪を低減するための1つの重要なテーマになると考えています。このテーマに取り組むことで、現実世界と同じく、サイバー空間においても安全・安心な社会の実現を目指します。

参考文献

- 1) We Are Social: The state of the Internet in Q2 2017, 2017.4
- 2) 総務省: 情報通信白書平成27年版, 2015.7
<http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/index.html>
- 3) Singapore Police Force: Annual Crime Brief 2015, 2016.2
- 4) Singapore Police Force: Annual Crime Brief 2016, 2017.2
- 5) NEC プレスリリース: NEC、米国国立機関による動画顔認証の性能評価で第1位を獲得, 2017.3
http://jpn.nec.com/press/201703/20170316_01.html
- 6) 越仲 孝文ほか: 音声・音響分析技術とパブリックソリューションへの応用, NEC技報 Vol.67 No.1, pp.86-89, 2014.11
- 7) K. Iwamoto, et al.: BRIGTH: A Scalable and Compact Binary Descriptor for Low-Latency and High Accuracy Object Identification, IEEE ICIP, 2013.9
<http://ieeexplore.ieee.org/document/6738600/>

執筆者プロフィール

谷 真宏

データサイエンス研究所
主任研究員

NEC 技報のご案内

NEC 技報の論文をご覧くださいありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）

NEC Technical Journal（英語）

Vol.70 No.2 ビジネスの安全・安心を支えるサイバーセキュリティ特集 ～Futureproof Security 安心の先へ。～

ビジネスの安全・安心を支えるサイバーセキュリティ特集によせて
増大するサイバー犯罪の根源的な解決へ～“産学官”のオールジャパンで立ち向かう第三者機関の姿とは？～
サイバーセキュリティを取り巻く社会動向とNECの取り組み

◇ 特集論文

社会の動向とNECの取り組み

重要インフラに対するサイバー攻撃の実態と分析
2017 サイバー攻撃最新動向 NEC Cyber Threat Intelligence 活用モデル
サイバーセキュリティ対策の社内事例

サイバーセキュリティソリューション

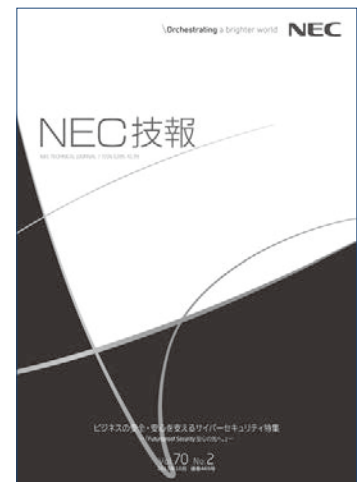
複雑化/高度化するサイバー脅威に対抗するSOCとセキュリティ監視サービス
攻撃被害を極小化するためのインシデント対応支援ソリューション
サイバー演習によるインシデントハンドリング能力の強化
セキュリティ統合管理・対処ソリューション「NEC Cyber Security Platform」
クラウド型ファイル暗号化サービス - ActSecure クラウドセキュアファイルサービス-
セキュリティLCMサービス
EMMを活用したセキュアなモバイルワークソリューション
IoT時代の経営を支援するサイバーセキュリティコンサルティング

サイバーセキュリティへのAI技術の活用

AI（人工知能）を活用した未知のサイバー攻撃対策
採るべき対策の「なぜ？」に答えるAIの可能性
オープンソースインテリジェンスを活用したサイバー脅威の検出と自動分析
犯罪捜査支援のためのサイバー・フィジカル統合分析技術

お客様に安全・安心を届けるための社内の取り組み

安全・安心な製品・サービスをご提供するための取り組み ～セキュア開発・運用～
サイバーセキュリティ人材のタレントマネジメント



Vol.70 No.2
(2017年10月)

特集TOP